Combining World Wide Web and wireless security

Joris Claessens, Bart Preneel and Joos Vandewalle
COmputer Security and Industrial Cryptography (COSIC)
Dept. of Electrical Engineering – ESAT, Katholieke Universiteit Leuven, Belgium
http://www.esat.kuleuven.ac.be/cosic/
joris.claessens@esat.kuleuven.ac.be

Keywords: WWW security, wireless security, m-commerce

Received: February 3, 2002

In current electronic commerce systems, customers have an on-line interaction with merchants via a browser on their personal computer. Also payment is done electronically via the Internet, mostly with a credit card. In parallel to this, e-services via wireless-only systems are emerging. This paper identifies security and functionality weaknesses in both of these current approaches. The paper discusses why and how general-purpose mobile devices could be used as an extension to PC based systems, to provide more security and functionality. General-purpose mobile devices are shown to be an alternative to costly special-purpose hardware. This combined approach has in many cases more interesting properties than when using mobile devices only. As an example of the combined approach, a GSM based electronic payment system is proposed and investigated. The system enables users to order goods through the World Wide Web and pay by using their mobile phone.

1 Introduction

In current electronic commerce systems, customers have an on-line interaction with merchants via a browser on their personal computer. Also payment is done electronically via the Internet, mostly by sending a credit card number to the merchant. This basic system is in widespread use today, and most people are familiar with buying books and music, booking flights, ordering PCs, etc. There are however some important security problems. For example, credit card numbers are often stolen by hackers from merchants' computers, orders and confirmations are usually not digitally signed and can be repudiated afterwards. In parallel to the fixed PC based systems, e-services are also emerging in the wireless world. Current mobile devices have however rather limited functionality, and in many applications, they are not suited to be used on their own.

This paper suggests a combined approach in which mobile devices are used as an extension to the World Wide Web environment. The paper starts with a description of the security properties of the World Wide Web in Sect. 2, and the security features in some wireless systems, i.e., GSM and WAP, in Sect. 3. Section 4 discusses security and functionality weaknesses in both worlds, and suggests a combined approach. An example of this approach is given in Sect. 5: a GSM based electronic payment system for the WWW is proposed and investigated. Further analysis of this system is presented in Sect. 6.

2 World Wide Web security

There are many security issues related to the WWW. Within the scope of this paper, we will only discuss the communications security aspect, both at the network and the application level, and the payment security aspect.

2.1 Communications security

The communication between a web browser and a web server is secured by the SSL/TLS protocol. Historically, Secure Sockets Layer (SSL) was an initiative of Netscape Communications. SSL 2.0 contains a number of security flaws which are solved in SSL 3.0. SSL 3.0 was adopted by the

IETF Transport Layer Security (TLS) working group, which made some small improvements and published the TLS 1.0 [9] standard. "SSL/TLS" is used in this paper, as "SSL" is an acronym everyone is quite familiar with; however, the use of TLS in applications is certainly preferred to the use of the SSL protocols.

Within the protocol stack, SSL/TLS is situated underneath the application layer. It can in principle be used to secure the communication of any application, and not only between a web browser and server. SSL/TLS provides entity authentication, data authentication, and data confidentiality. In short, SSL/TLS works as follows: public-key cryptography is used to authenticate the participating entities, and to establish cryptographic keys; symmetric key cryptography is used for encrypting the communication and adding Message Authentication Codes (MACs), to provide data confidentiality and data authentication respectively. Thus, SSL/TLS depends on a Public Key Infrastructure. Participating entities (usually only the server) should have a public/private key pair and a certificate. Root certificates (the certification authorities' certificates that are needed to verify the entities' certificates) should be securely distributed in advance (e.g., they are shipped with the browsers). Private keys should be properly protected. Note that these two elements, i.e., distribution of root certificates in browsers and the protection of private keys, is actually one of the weak and exploited points with respect to WWW security (see 4.1).

More detailed information on SSL/TLS, the security flaws in SSL 2.0, and the differences between SSL 3.0 and TLS 1.0, can be found in Rescorla [30].

2.2 Application security

SSL/TLS only protects data while it is in transit. Moreover, exchanged messages are not digitally signed. Therefore it does not provide non-repudiation. Both customers and merchants can always deny later on having sent or received requests or confirmations from each other.

In addition to SSL/TLS, critical messages should thus be digitally signed before they are sent through the secure channel. The concept of digitally signing messages is not really integrated yet in today's web browsers. Netscape though allows the content of forms to be digitally signed using the Javascript `signText()` function. XML will be more and more used on the WWW to represent content instead of the basic HTML. In the future, browsers are therefore expected to implement Signed XML [11], which specifies how XML documents should be digitally signed.

Note that an alternative protocol to secure the communication on the WWW has been proposed in the past: S-HTTP [31]. This protocol is situated at the application layer, and is specifically intended for HTTP. It secures HTTP messages in a very similar way to the protocols for secure email, and provides non-repudiation. SSL/TLS has however become the de-facto standard on the web, and S-HTTP was not a success.

2.3 Payment security

Although numerous different electronic payment systems have been proposed that can be or are used on the WWW, including micro-payment systems and cash-like systems, most transactions on the web are paid using credit cards. Mostly, customers just have to send their credit card number to the merchant's web server. This is normally done 'securely' over SSL/TLS, but some serious problems can still be identified. Users have to disclose their credit card number to each merchant. This is quite contradictory to the fact that the credit card number is actually the secret on which the whole payment system is based (note that there is no electronic equivalent of the additional security mechanisms present in real world credit card transactions, such as face-to-face interaction, physical cards and handwritten signatures). Even if the merchant is trusted and honest this is risky, as one can obtain huge lists of credit card numbers by hacking into (trustworthy, but less protected) merchants' web servers. Moreover, it is possible to generate fake but valid credit card numbers, which is of great concern for the on-line merchants. Thus, merchants bear risk in card-not-present transactions.

Secure Electronic Transaction, SET [33], is a more advanced standard for credit card based payments. One of its core features is that merchants only see encrypted credit card numbers, which can only be decrypted by the issuers. Moreover, the number is cryptographically bound to the transaction by a digital signature. This sys-

tem is conceptually much better, but until now it has not become popular due to its complexity.

Recently, Visa published the specifications of its 3-D Secure Authenticated Payment Program [37]. This system is mainly based on SSL/TLS. Its purpose is to authenticate cardholders in order to reduce the number of disputed on-line transactions.

American Express offers a 'one-time credit card' solution [1] with which customers can protect their privacy, but which also solves some of the above mentioned problems. Alternatively, several similar systems exist (e.g., InternetCash [18]) in which customers can obtain some pre-paid value identified and protected with a number and PIN, and use it on-line in cooperation with a central server. Finally, real-life electronic payment means (e.g., Proton [29] and debit cards) are also starting to be deployed on the WWW (e.g., [2]).

3 Wireless security

GSM and WAP are currently probably the two most popular and widely used wireless technologies. They are briefly presented in the following paragraphs. Thereafter, some other systems and initiatives in the wireless world are discussed.

3.1 GSM

GSM, Global System for Mobile communications, is the currently very popular digital cellular telecommunications system specified by the European Telecommunications Standards Institute (ETSI). In short, GSM intends to provide three security services [36]: temporary identities, for the confidentiality of the user identity; entity authentication, that is, to verify the identity of the user; and encryption, for the confidentiality of user-related data (note that data can be contained in a traffic channel, e.g., voice, or signaling channel, e.g., SMS messages).

The Subscriber Identity Module (SIM) is a security device, a smart card which contains all the necessary information and algorithms to authenticate the subscriber to the network. It is a removable module and may be used in any mobile equipment [36]. Note that the encryption algorithms are integrated into the mobile equipment as dedicated hardware. GSM does not use public-key cryptography. Symmetric keys are derived from user related data using an algorithm under the control of a master key.

The electronic payment system described in the example later in this paper, requires the SIM to contain a small payment application, based on the SIM Application Toolkit. The *SIM Application Toolkit* [14] provides mechanisms which allow applications, existing in the SIM, to interact and operate with any compliant mobile equipment. These mechanisms include displaying text from the SIM to the mobile phone, sending and receiving SMS messages, and initiating a dialogue with the user. In addition to the GSM security mechanisms, special SIM Application Toolkit security features have been defined [12, 13]. The security requirements that have been considered are: (entity) authentication, message integrity, replay detection and sequence integrity, proof of receipt and proof of execution, message confidentiality, and indication of the security mechanisms used. According to the standard, digital signatures can be used to implement some of these requirements.

Note that the same distinction between communications security and application security as made in the WWW security context, can be made here: standard GSM security at the communications level, and SIM Application Toolkit security at the application level.

3.2 WAP

The Wireless Application Protocol (WAP) is a protocol stack for wireless communication networks. WAP is bearer independent; the most common bearer is currently GSM.

Similar to SSL/TLS for the Internet, WTLS [44] is WAP's communications security solution. It also relies on a Public Key Infrastructure [40, 39]. The main differences are that WTLS supports by default algorithms based on elliptic-curve cryptography, is adapted for datagram communication (instead of connection), and supports its own certificate format, besides X.509v3, optimized for size. TLS was as such modified to make it more suitable in an environment where there are bandwidth, memory, and processing limitations.

At the application layer, WAP provides digital signature functionality through the WMLScript Crypto Library [45], which is similar to Netscape's

Javascript signing. Comparable to the GSM's SIM, WAP devices will use a Wireless Identity Module (WIM) [43] which can contain the necessary private and public keys to perform digital signatures and certificate verification respectively.

3.3 Other systems and inititiatives

GSM is a second-generation system (2G). UMTS, Universal Mobile Telecommunications System [35], is part of a global family of third-generation (3G) mobile communications systems. These systems provide high-capacity and more secure [38] communication. A competitor of WAP is NTT DoCoMo's i-mode [27]. Bluetooth [5] is a wireless protocol for communication between devices that are in close proximity. The Internet itself is also expanding to the wireless world. The IETF is currently defining standards for Mobile IP [17], and is working on extensions (including wireless) for TLS [4].

The Mobile Electronic Signature Consortium has defined mSign [24], which should provide a standardized interface between Primary Service Providers (e.g., merchants) and Mobile Operators. It allows Primary Service Providers to request signatures from end-users through the Mobile Operators. The Mobile electronic Transactions initiative – MeT [25] – intends to establish a consistent and coherent framework for secure mobile transactions, based on existing standards and specifications; where needed, new functionality will be submitted to relevant standardization and specification organizations. There are numerous other fora concerned with mobile secure payments, see [7] for a description and comparison of these.

4 Combining WWW and wireless

Both the World Wide Web and the wireless world on their own have security and/or functionality problems. These shortcomings are explained in the following paragraphs. An approach in which the two worlds and their advantages are combined, is then motivated.

4.1 WWW: problems

It is very common that only web servers have certificates with which they are authenticated. In case user authentication is needed, it is almost never done via SSL/TLS client authentication. Users are often authenticated via their IP address, which is vulnerable to IP spoofing [3], which certainly does not provide mobility, and which is just not usable in an open system. Fixed passwords are frequently used, which provide mobility, but which are vulnerable to guessing, dictionary attacks and social engineering [26]. Passwords that are only used once [21] are not frequently used. They would be more secure, but certainly less convenient.

Root certificates are needed when verifying a web server certificate. It is very important that a user has an authentic copy of these certificates. This is more or less ensured by shipping them together with the browsers. It is however easy to add more or even replace root certificates. Moreover, the browser trust model causes a server certificate to be trusted if it is successfully verified by any of the root certificates (since there is usually no central policy management, this might easily include an attacker's root certificate). Finally, browsers generally also do not yet check by default if a certificate has been revoked.

Users must recognize when they have a secure session with a web server. However, in todays browsers, there are only some limited visual indications (e.g., closed lock), and an unexperienced user is easily fooled by a spoofed web site as demonstrated by Felten *et al.* [15] and more recently by Yuan *et al.* [46].

If the user has a public/private key pair – for SSL/TLS client authentication, for SET, or for digitally signing documents – the private key will mostly reside on the hard disk of the machine. Even if it is protected by a pass phrase, it is still very vulnerable, for example due to Trojan horses. Users with such a software token are also hardly mobile. Smart cards are a solution, but for particular applications, they might be inconvenient. Moreover, smart card readers are currently not installed on each machine. Other special-purpose hardware, such as a Digipass [10], as sometimes used in e-banking, might be too costly for small applications, i.e., the investment for the customers and/or merchants would just be too

high compared to the expected benefits.

Current end-user computing systems tend to offer more functionality at the cost of security. This is actually the reason why for example root certificates and private keys are so vulnerable on current end-user machines. Specifically, there is currently a lack of secure operating systems [22] and trusted components [34]. Today's PC and browser offer advanced functionality, but are (therefore) an insecure environment.

4.2 Wireless: problems

While the security problems on the WWW are currently more related to the secure management of the end-points, the security problems in some wireless systems are still with the protocols and algorithms themselves. For example, algorithms used by many GSM providers have been broken and 'over-the-air cloning' and real-time eavesdropping have been shown (at least in theory) to be feasible [32]. Security problems have been discovered in other mobile systems too [6, 19]. Most of these problems are due to non-public design of the algorithms and protocols, leakage and/or publication of the details to the general public afterwards, and discovery of flaws by the cryptographic community.

More conceptually, both GSM and WAP do not offer end-to-end security. GSM security only applies on the wireless link, i.e., from mobile phone to base station, but not from mobile phone to mobile phone. The fixed network is considered to be secure (more precisely, GSM intends to offer the same security level as the fixed network). In the WAP architecture, WAP devices communicate with web servers through a WAP gateway. WTLS is only used between the device and the gateway, while SSL/TLS can be used between the gateway and the server. From a security point of view, this means that the gateway should be considered as a person-in-the-middle. Note that WAP is now evolving into end-to-end security [42, 41].

Security seems to evolve in the good direction though. From a usability point of view on the other hand, mobile devices have still a rather limited functionality. They are not performant, and have often a quite poor human-device interface. Although mobile devices are getting more advanced, they will always be outsmarted by desktop PCs. Note that the complexity of the PC (e.g., multi-user operating system, data with executable content, ...) is the main reason why securing the end-points of the communication is such a difficult task, and remains an important problem on the WWW. As long as mobile devices stay quite simple and do not provide too much functionality, their security as an end-point will be more easy to cope with.

4.3 Motivation for a combined approach

By combining the World Wide Web with a wireless system, we want to come to practical and low-cost electronic commerce applications, which can fully exploit the broad functionality of the WWW. Two goals should hereby be achieved at the same time: *security* and *mobility*.

The WWW on its own does not seem to be sufficient for these applications. It surely provides broad functionality. When for example only fixed passwords are used, the WWW also offers mobility, i.e., a user can initiate transactions from any computer (e.g., a public terminal). Strong security is in that case however not achieved. Stronger security can be achieved by using for example cryptographic keys stored on the computer's hard disk. However, this does not allow for practical mobility. Special-purpose hardware tokens would increase the security of the application and provide mobility again. However, in an electronic commerce environment, consumers do not likely want to pay for a token that can only be used in the context of that application.

Wireless systems on their own are not suitable either. By definition, they offer mobility. Although there are some weaknesses in current systems, security in wireless systems tends to improve substantially. It is however clear that the GSM system is a rather limited environment. WAP offers a more general and WWW-like functionality, but in practice today's devices and networks do not satisfy the needs of merchants and customers. Mobile devices are generally expected to stay inferior to desktop computers.

This brings us to the motivation for a combined approach. Mobile devices are general-purpose devices which can be used as an extension to the WWW – instead of special-purpose devices – to offer more security and mobility without any ex-

tra cost. These mobile devices can be personalized and can store secret information such as cryptographic keys. They can be used in combination with any computer, i.e., the personal computer at the user's home, but also a public terminal, hereby providing mobility. Moreover, the computer terminal must not necessarily be completely trusted, as (part of) the security will rely on trusted and/or secret information that is securely stored in the device (and never leaves it, in case of secrecy).

In the remainder of this paper, this combined approach will be illustrated with an electronic payment system for the WWW that makes use of a mobile phone. This GSM based system is an alternative to the widely spread credit card based solution, offering more security and equivalent mobility and complexity (assuming that a mobile phone is standard equipment of many users). In addition, it might be suited for lower-price transactions.

5 GSM based payment for the WWW

The main goal of the remaining part of the paper is to present a system in which the WWW and GSM environment are combined to improve overall security, mobility, and functionality. In particular, an architecture and protocol are developed in which: (1) a customer can initiate and complete an electronic *payment* over the GSM network where the network operator is an active participant; (2) the *pre-payment* related interaction is done via the WWW; (3) the customer receives a receipt with which he/she can pick up the goods (*post-payment*).

5.1 Involved entities

The following entities play an active role in this e-commerce system:

Customer The Customer wants to buy something via the WWW. Payment will be done via his/her GSM. The Customer will receive a receipt, with which he/she can pick up the goods (the system must work with both physically deliverable goods and electronically available goods). Obviously, the Customer should have a PC with Internet connection. This can also be a public terminal. He/she needs a mobile phone with SIM Application Toolkit functionality. The SIM card should be issued by a Network Operator that is running this electronic payment service. Optionally, there should be a connection between the mobile phone and the PC, and accordingly some extra software on the PC.

Merchant The Merchant wants to sell something via the WWW. He/she should have a web server, and an access point to the mobile network. Examples are an on-line bookstore, a pizza delivery chain, an electronic parts shop, etc.

Deliverer The Deliverer is the local (with respect to the Customer) representative of the Merchant. It will deliver the goods after having verified the receipt the Customer has obtained from the Merchant. The Deliverer should have some equipment to verify this receipt. An example is the pizza delivery boy/girl, etc. The Deliverer can also be another company that made an agreement with the Merchant. For example, the Merchant can send the goods to a gas station near the Customer; in this case, the gas station is the Deliverer where the Customer can pick up the goods.

Network Operator The N.O. plays the role of the bank. It will deduct the necessary amount of money from the Customer's balance (can be credit or pre-payment based), and add this amount to the Merchant's balance. A commission on this amount will be taken, or a periodical fee will be requested from the Customer and/or Merchant. In practice there will be multiple N.O.s: N.O.(C), N.O.(M) and N.O.(D), for the Customer, the Merchant and the Deliverer respectively (as shown in Fig. 1).

Note that in reality, and from a non-technical point of view, it might not be easy for any Network Operator to deploy an electronic payment service (e.g., banking license). Alternatively, the "Network Operator" could in this system be replaced by a real financial institution, which makes an agreement with one or more operators.

5.2 Architecture and protocol

From a high-level point of view, the different entities perform the following interactions (see Fig. 1): after browsing and negotiating, the Customer requests a purchase; via an SMS message, the Merchant asks the Customer to pay the purchase; the Customer pays by sending an SMS message to the Network Operator; the Network Operator informs the Merchant about the successful payment; the Merchant sends a receipt to the Customer (also an SMS message); the Customer can use this receipt to pick up the goods at the Deliverer.

The protocol contains the following steps (see Fig. 1):

1. Purchase Request After browsing and negotiating (0), the Customer makes a *Purchase Request* via the WWW (1). The Merchant can choose the format and encoding of the message. It should at least contain a description of the goods, the amount of money to be paid, and the Customer's GSM number (in order to be able to send an SMS message to the Customer). The message will normally be sent through submission of an HTML form. The level of protection can be chosen by the Merchant, but it will normally be protected in transit by SSL/TLS. The form could also be digitally signed by the Customer (e.g., Netscape's Javascript signing capability, or Signed XML).

2. Purchase Confirm The Merchant sends a *Purchase Confirm* via SMS (2) to the Customer's mobile phone. This message should be in a standard format, and is optionally digitally signed by the Merchant. The message contains: (optionally) a description of the goods (either a hashed form of the description, or an abbreviated yet unique description of the goods, e.g., as in supermarket receipts), a Transaction ID (TID), a unique Merchant ID, the ID of N.O.(M), and the amount of money to be paid. The Merchant also sends a *Purchase Confirm* via the WWW (2). Note that this could already be included in the reply to the submission of the Purchase Request form.

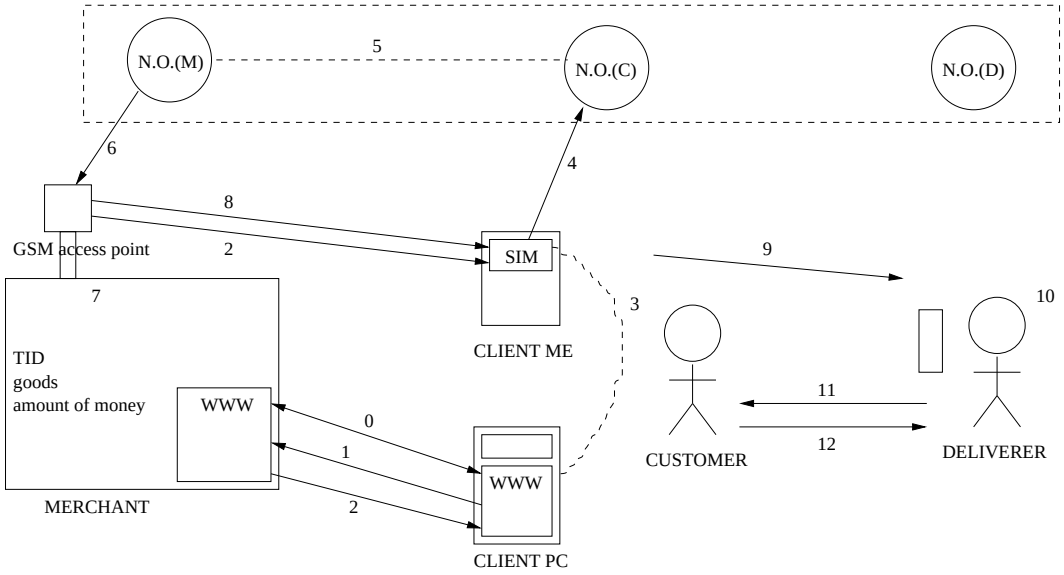
3. Verification by the Customer The Customer verifies whether all the ordered goods are listed, and whether the amount of money requested equals the amount agreed on. The information in the SMS message should be the same as the information displayed in the browser. Authentication of the Merchant thus relies on both GSM (we assume that the Customer knows the number of the Merchant) and SSL/TLS, so the Customer's trust in the correct execution of the transaction increases. If the reply in the browser and/or the SMS message are digitally signed, the signatures are verified. Note that in current GSM phones such a signature must possibly be verified using additional software on the computer. This requires a connection between the mobile phone and the PC which can for example be provided by Bluetooth. An automatic verification and comparison of the reply in the browser and the SMS message can then also be made. The interface to the Customer is provided by the SIM Application Toolkit. A payment application is installed on the SIM card, which is invoked on receipt of a Purchase Confirm message.

4. Debit Account The SIM Application Toolkit application asks the Customer a confirmation for sending a *Debit Account* message (4) to the N.O.(C). This message includes the amount of money to be paid, the TID, the Merchant's ID and N.O.(M)'s ID. The authentication of the Customer relies on GSM entity authentication (the Customer's mobile phone number should be in the Merchant's database). The TID will allow verification by the Merchant afterwards.

5. Inter-N.O The N.O.(C) deducts the proper amount of money from the Customer's balance, and forwards the Debit Account message to N.O.(M). The N.O.(M) adds the amount to the Merchant's account.

6. Delivery OK The N.O.(M) sends a *Delivery OK* (6) to the Merchant. This message contains the amount of money and the TID, and can be digitally signed by the N.O.(M).

7. Verification by the Merchant The Merchant verifies if the *Delivery OK* message originates from the N.O.(M) (relying on GSM entity authentication). If added, the digital signature of the N.O.(M) is verified. The Merchant looks up



1. Purchase Request
2. Purchase Confirm
3. Verification by Customer
4. Debit Account
5. Inter-N.O.
6. Delivery OK
7. Verification by Merchant
8. Receipt
9. Presentation of Receipt
10. Verification by Deliverer
11. Delivery of Goods
12. Confirmation of Reception

Figure 1: GSM based payment for the WWW: architecture and protocol

the TID in his transaction database, and checks if the amount of money is the same as included in the corresponding Purchase Confirm messages.

8. Receipt The Merchant sends a *Receipt* (8) to the Customer via SMS. It contains: a (hashed) description of the goods, the TID, a timestamp (in order for the Deliverer to verify the freshness of the receipt), information on the Deliverer (optionally depending on the Customer's cell location, and including the Deliverer's GSM number), and information on the Customer (optionally including its GSM number, to allow verification of ownership of the receipt). The receipt is digitally signed by the Merchant. The receipt can only be used for the intended Deliverer as indicated. The TID and timestamp ensure that the receipt cannot be replayed by the Customer (i.e., the Deliverer should keep a list of previously received TIDs and should not accept receipts that are too old). GSM authentication is relied upon for authenticating the Customer.

9. Presentation of the receipt If goods are electronic and delivered via the WWW, a receipt is not needed. Goods are then downloaded using the TID. The Merchant keeps a list of which TIDs correspond to transactions for which a payment has been received. Physical goods should be retrieved at the Deliverer. The receipt is forwarded to the Deliverer (9), manually or through the SIM Application Toolkit, or the Customer just presents the receipt to the Deliverer on the screen of his/her own GSM.

10. Verification by the Deliverer The Deliverer just reads the receipt from the screen of the Customer's or his/her own GSM, or he/she verifies the receipt more properly by checking if the signature of the Merchant is valid. The Deliverer needs some infrastructure with GSM access point for this (e.g., a GSM connected to a laptop).

11. Delivery of goods If the receipt is valid, the Deliverer can be sure that the Customer is the one that has made (and paid) the purchase. The goods can thus be delivered (11). In case of

electronic goods which are delivered directly by the Merchant's web site (not necessarily though, as the Deliverer might have its own web site), the Customer should be granted access based on the TID: after a Delivery OK message has been received, the Merchant enables the access to the information; the TID should not be known to other entities (however, note that the N.O. should be trusted not to misuse its knowledge of the TID).

12. Confirmation of reception After the Customer has obtained the goods, it can optionally be required that he/she confirms the reception of the goods (12), e.g., by digitally signing a specific message. This will prevent Customers from denying later on having received the goods.

6 Analysis and remarks

The proposed GSM based electronic payment system for the WWW is analyzed further in this section. Some GSM specific comments are given, the security and privacy of the system is evaluated, and a comparison with a number of similar systems is made. Note that this section only intends to discuss this particular example, and not the general combined approach.

Only the essential steps of the proposed payment system are presented in this paper. It is clear that a real implementation of this system would require many extra features. For example, it is possible that the Customer completed the payment but did not receive a receipt. Other kinds of interrupted transactions might occur. To be able to cope with this, status and cancel requests should be built into the system.

6.1 GSM functionality

The protocol relies on SMS messages. These can only contain 160 characters, which should be taken into account when defining the exact content of the protocol messages. Note that GSM provides a mechanism to send long messages as a concatenation of multiple SMS messages. Since the protocol involves on-line bi-directional communication between the entities, there should be not much latency between sending and receiving SMS messages. This might be a problem in the case of international roaming.

The proposed system relies on GSM authentication. The participants can only verify the identity of their communication peers though if "caller identification" is supported by the mobile network and the phone, and if it is not disabled.

6.2 Security

The security features of SSL/TLS and GSM form together a basis for the security of the proposed electronic payment system. By having a close link between the two, the security is even improved.

The Customer can securely request a purchase via SSL/TLS. The Customer will receive a confirmation via this same secure channel, and also on its mobile phone. Therefore, the Customer can double-check the Merchant's identity, and the contents of the purchase, including the amount of money to be paid.

The Merchant can rely on the GSM network to be sure to receive an authenticated payment from the Customer via the Network Operator later on. Moreover, the Customer cannot cheat by requesting its Network Operator to deduct a smaller amount of money than originally requested by the Merchant. The Merchant would notice the smaller amount of money and not send a receipt.

The Deliverer can validate a receipt by verifying the digital signature of the Merchant, and by checking if the receipt is fresh. Thus, receipts cannot be forged, and cannot be replayed. Moreover, if the Customer's mobile phone number is included in the receipt, the Deliverer could rely on GSM authentication and check if the receipt is actually presented by the original initiator of the transaction (note that for some applications, Customers might desire to be able to forward the receipt to another party that in its turn can pick up the goods).

As on top of SSL/TLS and GSM, some crucial messages are digitally signed; this decreases the need for Customers and Merchants to trust each other (i.e., they only need to trust they use the right public key, which should be ensured by the certificates that are issued by mutually trusted CAs). For example, since the receipt is digitally signed, it cannot only be verified by the Deliverer, but also by a Judge, in case of a dispute. Note that the latter also requires that the receipt includes a unique and indisputable description of the goods that should be delivered.

The Network Operator is trusted to transfer the proper amount of money from the Customer's to the Merchant's balance. It is expected to do so, as its business would otherwise quickly collapse due to negative publicity.

In some sense, the Customer's mobile phone can be considered as a secure and personal device (and care should therefore be taken that it is not easily stolen or lost). The strength of the electronic payment system proposed in this example relies particularly on the security of such a device, which is combined with the advanced yet insecure environment provided by the PC and the browser.

6.3 Privacy

The presented electronic payment system seems to offer more security than today's widely used mechanisms; however, it does not really offer more privacy. Merchants know at least the mobile phone number of their Customers. This number does not necessarily reveal a Customer's real identity (as opposed to an ordinary credit card payment). There already exist phone books with GSM numbers though. One would for example certainly not be happy when this number would be used for advertisement purposes. In fact, for this reason, some people will be reluctant to release their phone number, while they freely disclose their credit card number to merchants. The ability of hiding numbers or anonymizing customers in another way, would thus be an improvement of the system. Just as with credit card payments, the Network Operator knows exactly which Customers are buying goods from which Merchants and for what amount of money. The Network Operator will not necessarily know the actual nature of the goods though.

6.4 Other approaches

Numerous other GSM based payment systems exist. GiSMo [16] is (was) a system intended for the Internet in which customers receive a random code through SMS via a central server. This random code is then entered via the computer in order to pay. Mint [23] is a system in which each terminal/shop has a unique phone number which the customer should just call at the time of payment. Similar alternatives are Jalda [20] and Paybox [28].

In the system presented in this paper, more payment related information is exchanged via GSM, which results in a closer link between the WWW and the GSM interaction. Conceptually, it is also more general and independent of the wireless system. With more advanced mobile devices and networks, such as UMTS, more secure schemes would be possible, following the same architecture and protocol, but with different content of (and another exchange mechanism of) the messages. For example, instead of an account based protocol, electronic cash like schemes could be used. Mobile devices with built-in smart card readers would be very useful for integrating smart card based payment means as used in the physical world.

7 Conclusion

Electronic commerce is already a normal part of people's ordinary life. Mobile devices, and certainly mobile phones, are currently widely spread. This paper gave a brief overview of the security properties of the World Wide Web and some existing mobile systems. The main purpose of this paper was to suggest to use a wireless system as an extension to the WWW, to provide more security and functionality. To demonstrate this combined approach, a GSM based electronic payment for the WWW was presented.

Unlike most mobile phones, some mobile devices are powerful and advanced enough to allow more or less convenient browsing and shopping. Future mobile systems will also be more secure and will offer more functionality than the GSM system or than WAP. Yet, the concept of using an out-of-band channel for electronic payment, and the combined use of a mobile device together with a normal PC, will remain very useful. For the PC and its big screen will always be far more advanced than the mobile device, but will never be mobile.

Acknowledgements

Joris Claessens is funded by a research grant of the Institute for the Promotion of Innovation by Science and Technology in Flanders (IWT). This work was also partially supported by the Con-

certed Research Action (GOA) Mefisto-666 of the Flemish Government.

This work was mainly initiated during a research visit at the Information Security Research Centre (ISRC) of Queensland University of Technology (QUT), Brisbane, Australia. The first author wants to thank Dr. Mark Looi of the ISRC for the interesting discussions on this topic. The authors also want to thank Dr. Silke Holtmanns of Ericsson for the various pointers to existing mobile payment systems.

An earlier version of this article was presented at and published in the proceedings of the IFIP I-NetSec'01 conference [8]. The authors want to acknowledge the anonymous reviewers for their constructive remarks and suggestions.

References

[1] American Express. Private Payments. http://www.americanexpress.com /private-payments/.

[2] Banxafe. http://www.banxafe.com/.

[3] Steven M. Bellovin. Security Problems in the TCP/IP Protocol Suite. *Computer Communication Review*, 19(2):32–48, April 1989.

[4] Simon Blake-Wilson, Magnus Nystrom, David Hopwood, Jan Mikkelsen, and Tim Wright. TLS Extensions. IETF Internet Draft, December 2001.

[5] Bluetooth. http://www.bluetooth.com/.

[6] Nikita Borisov, Ian Goldberg, and David Wagner. Intercepting Mobile Communications: The Insecurity of 802.11. In *Proceedings of the 7th ACM Annual International Conference on Mobile Computing and Networking*, pages 180–189, 2001.

[7] Clara Centeno. Mobile Payment Industry Fora – Consolidation of Initiatives Expected. *Electronic Payment Systems Observatory – Newsletter, ePSO–N*, (8):8–12, July 2001. Available at http://epso.jrc.es/.

[8] Joris Claessens, Bart Preneel, and Joos Vandewalle. Combining World Wide Web and wireless security. In Bart De Decker, Frank Piessens, Jan Smits, and Els Van Herreweghen, editors, *Advances in Network and Distributed Systems Security – Proceedings of IFIP I-NetSec'01*, pages 153–171. Kluwer Academic Publishers, 2001.

[9] Tim Dierks and Christopher Allen. The TLS Protocol Version 1.0. IETF Request for Comments, RFC 2246, January 1999.

[10] Digipass. http://www.vasco.com/.

[11] Donald Eastlake, Joseph Reagle, and David Solo. XML-Signature Syntax and Processing. IETF Request for Comments, RFC 3075, March 2001.

[12] ETSI. Digital cellular telecommunications system (Phase 2+); Security mechanisms for the SIM Application Toolkit; Stage 1. ETSI TS 101 180 (GSM 02.48).

[13] ETSI. Digital cellular telecommunications system (Phase 2+); Security mechanisms for the SIM Application Toolkit; Stage 2. ETSI TS 101 181 (GSM 03.48).

[14] ETSI. Digital cellular telecommunications system (Phase 2+); Specification of the SIM Application Toolkit for the Subscriber Identity Module – Mobile Equipment (SIM – ME) interface. ETSI TS 101 267 (GSM 11.14).

[15] Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Web Spoofing: An Internet Con Game. In *Proceedings of the 20th National Information Systems Security Conference*, pages 95–103, 1997.

[16] GiSMo. Was available at http://www.gismo.net/, but is currently withdrawn by Millicom International Cellular S.A.

[17] IETF Working Group. IP Routing for Wireless/Mobile Hosts (mobileip).

[18] InternetCash. http://www.internetcash.com/.

[19] Markus Jakobsson and Susanne Wetzel. Security Weaknesses in Bluetooth. In D. Naccache, editor, *Topics in Cryptology – Proceedings of the Cryptographers' Track at RSA 2001*, Lecture Notes in Computer Science,

LNCS 2020, pages 176–191. Springer-Verlag, 2001.

[20] Jalda. http://www.jalda.com/.

[21] Leslie Lamport. Password Authentication with Insecure Communication. *Communications of the ACM*, 24(11):770–772, November 1981.

[22] Peter A. Loscocco, Stephen D. Smalley, Patrick A. Muckelbauer, and Ruth C. Taylor. The Inevitability of Failure: The Flawed Assumption of Security in Modern Computing Environments. In *Proceedings of the 21st National Information Systems Security Conference*, pages 303–314, October 1998.

[23] Mint. http://www.mint.nu/.

[24] Mobile Electronic Signature Consortium. http://www.msign.org/.

[25] Mobile electronic Transactions. http://www.mobiletransaction.org/.

[26] Robert Morris and Ken Thompson. Password Security: A Case History. *Communications of the ACM*, 22(11):594–597, 1979.

[27] NTT DoCoMo. i-mode. http://www.nttdocomo.co.jp/.

[28] Paybox. http://www.paybox.de/.

[29] Proton. http://www.protonworld.com/.

[30] Eric Rescorla. *SSL and TLS: Designing and Building Secure Systems*. Addison-Wesley, 2000.

[31] Eric Rescorla and Allan M. Schiffman. The Secure HyperText Transfer Protocol. IETF Request for Comments, RFC 2660, August 1999.

[32] Bruce Schneier. European Cellular Encryption Algorithms. *Crypto-Gram*, December 1999.

[33] SET Secure Electronic Transaction LLC. SET Secure Electronic Transaction Specification. http://www.setco.org/.

[34] TCPA. Trusted Computing Platform Alliance. http://www.trustedpc.org/.

[35] The UMTS Forum. http://www.umts-forum.org/.

[36] Klaus Vedder. GSM: Security, Services and the SIM. In B. Preneel and V. Rijmen, editors, *State of the Art in Applied Cryptography*, Lecture Notes in Computer Science, LNCS 1528, pages 227–243. Springer-Verlag, 1998.

[37] Visa. 3-D Secure Authenticated Payment Program. http://international.visa.com/.

[38] Mike Walker. On the security of 3GPP networks. Invited talk at Eurocrypt 2000.

[39] Wireless Application Protocol Forum. WAP Certificate and CRL Profiles. Approved 22-May-2001.

[40] Wireless Application Protocol Forum. WAP Public Key Infrastructure. Version 24-Apr-2001.

[41] Wireless Application Protocol Forum. WAP TLS Profile and Tunneling. Version 11-April-2001.

[42] Wireless Application Protocol Forum. WAP Transport Layer End-to-end Security. Approved Version 28-June-2001.

[43] Wireless Application Protocol Forum. WAP Wireless Identity Module, Part: Security. Version 12-July-2001.

[44] Wireless Application Protocol Forum. WAP Wireless Transport Layer Security. Version 06-Apr-2001.

[45] Wireless Application Protocol Forum. WAP WMLScript Crypto Library. Version 20-Jun-2001.

[46] Yougu Yuan, Eileen Zishuang Ye, and Sean Smith. Web Spoofing 2001. Department of Computer Science, Dartmouth College, Technical Report TR2001-409, July 2001.